



**Privacy Impact Assessment Update
for the
Electronic System for Travel
Authorization (ESTA)**

DHS/CBP/PIA-007(d)

November 3, 2014

Contact Point

Suzanne Shepherd

Director - ESTA

U.S. Customs and Border Protection

(202) 344-3710

Reviewing Official

Karen L. Neuman

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

The Electronic System for Travel Authorization (ESTA) is a web-based application and screening system used to determine whether certain foreign nationals are eligible to travel to the United States under the Visa Waiver Program. The U.S. Department of Homeland Security, U.S. Customs and Border Protection is publishing this update to the Privacy Impact Assessment (PIA) for ESTA, last updated on June 5, 2013, to provide notice of changes to the ESTA application questionnaire and expansion of the ESTA application data elements.

Overview

In the wake of the terrorist attack on the Nation on September 11, 2001, Congress enacted the Implementing Recommendations of the 9/11 Commission Act of 2007.¹ Section 711 of that Act sought to address the security vulnerabilities associated with Visa Waiver Program (VWP) travelers who are not subject to the same degree of screening as other international visitors to the United States. As a result, section 711 requires DHS to develop and implement a fully automated electronic travel authorization system to collect biographical and other information necessary to evaluate the security risks and eligibility of an applicant to travel to the United States under the VWP. The VWP is a travel facilitation program that has evolved since the September 11 terrorist attack to include more robust security standards that are designed to prevent terrorists and other criminal actors from exploiting the Program to enter the country.

ESTA is a web-based system that DHS/CBP developed in 2008 to determine the eligibility of foreign nationals to travel to the United States under the Visa Waiver Program (VWP) by air or sea. Applicants submit biographic information and answer eligibility questions using the ESTA website. Information collected by ESTA is necessary to issue a travel authorization as reflected on the Form I-94W.² In the air and sea environments, a VWP traveler who intends to arrive at a U.S. air or sea port of entry must currently obtain an approved travel authorization via the ESTA website prior to boarding a carrier bound for the United States. The development of the ESTA program has allowed the Department to eliminate the requirement that VWP travelers complete a Form I-94W prior to being admitted to the U.S. at an air or sea port of entry because the ESTA application electronically captures duplicate biographical and travel data elements collected on the paper Form I-94W.

CBP uses the information submitted to ESTA to make a determination whether the applicant's intended travel poses a law enforcement or security risk. CBP vets the ESTA applicant information against selected security and law enforcement databases at DHS, including

¹ Pub. L. 110-53, codified at 8 U.S.C. § 1187(a)(11), (h)(3), available at, <http://www.gpo.gov/fdsys/pkg/PLAW-110publ53/html/PLAW-110publ53.htm>.

² See 8 CFR § 217.5(c). The Form I-94W must be completed by all nonimmigrant visitors not in possession of a visitor's visa, who are nationals of one of the VWP countries enumerated in 8 CFR 217.



but not limited to TECS (not an acronym)³ and the Automated Targeting System (ATS).⁴ ATS also retains a copy of ESTA application data to identify potential high-risk ESTA applicants.

DHS may also vet ESTA application information against other federal security and law enforcement databases to enhance DHS's ability to determine whether the applicant poses a security risk to the United States or is eligible to travel to and enter the United States under the Visa Waiver Program. The ESTA eligibility determination is made prior to a visitor boarding a carrier en-route to the U.S.

Reason for the PIA Update

In response to the deteriorating security situation in Iraq and Syria, and the increasing concerns regarding the potential exploitation of VWP travel by foreign fighters, DHS/CBP is strengthening the security of the VWP through enhancements to ESTA. DHS has determined that ESTA enhancements will improve the Department's ability to screen prospective VWP travelers and more accurately and effectively identify those who pose a security risk to the U.S. DHS also believes enhancements to ESTA will help the Department facilitate adjudication of ESTA applications by reducing the number of inconclusive matches.

Therefore, DHS/CBP is amending the ESTA application to include additional data fields for all new and renewal ESTA applications beginning October 1, 2014.⁵ DHS/CBP is also revising the eligibility questions on the ESTA application to simplify and clarify them. By requiring ESTA applicants to provide additional information, DHS enhances its ability to identify those applicants who pose a potential security threat to the United States, including known or suspected terrorists. This additional information will also help reduce the number of inconclusive matches that currently result in an ESTA denial (which in turn requires the applicant to apply for a B1/B2 nonimmigrant visa for travel to the United States).

DHS must be agile and vigilant in continually adapting to evolving threats and hazards. Specifically, the inclusion of additional data fields on the ESTA application will provide a greater chance for DHS to identify foreign fighters with passports from VWP countries before they attempt to travel to the U.S.

ESTA Enhancement Data Elements

Effective October 1, 2014, the following data elements will be added to the ESTA web form for all new and renewal ESTA applications:

³ See DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, published December 22, 2010.

⁴ See DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, published June 1, 2012.

⁵ Approved ESTA applications are valid for two years, or until the passport expires, whichever comes first. Approved ESTA applications support multiple trips a traveler may make to the United States without having to re-apply for another ESTA. . See "About the Electronic System for Travel Authorization (ESTA,)" for more general ESTA information, available at <http://www.cbp.gov/travel/international-visitors/esta>.



- Other Names or Aliases
- Other Country of Citizenship
 - If yes, passport number on additional citizenship passport
- City of Birth
- Home Address
- Parents' Names
- Email
- Telephone Number
- National Identification Number
- Current Job Title
- Current or Previous Employer Name
- Current or Previous Employer Address
- Current or Previous Employer Telephone Number
- Emergency Point of Contact Information Name
- Emergency Point of Contact Information Phone
- Emergency Point of Contact Information Email
- U.S. Point of Contact Name
- U.S. Point of Contact Address
- U.S. Point of Contact Telephone Number

Eligibility Questions

This PIA is also being updated to reflect the revised eligibility questions that new applicants must complete on the ESTA application. While the substance of the revised eligibility questions remain similar to the previous questions, a number of the questions have been reworded in “plain language” to make the questions easier to understand by the general public, and travelers for whom English is not the first language. For example, previous questions asking whether an applicant has been arrested or convicted of a crime of moral turpitude or has been involved in persecutions associated with Nazi Germany have been reworded to elicit more general information about criminal or terrorist history. CBP also removed confusing and archaic language to promote readability and make the ESTA application online more user-friendly.

U.S. Person Information

DHS is providing express notice that U.S. citizens, U.S. businesses or entities, or Lawful Permanent Residents (LPR), hereinafter “U.S. Persons,” information will now be collected and maintained in ESTA. Though DHS already extends certain Privacy Act protections to “mixed



systems” (systems that contain U.S. citizen, LPR, and foreign national information)⁶ and DHS has always deemed ESTA to be a “mixed system,” the updated ESTA information collection will now include information about U.S. Persons. U.S. Person information could be provided for the following fields in the ESTA application: Parents’ Names; Current or Previous Employer Name or Address; U.S. Point of Contact Name or Address; Emergency Point of Contact Name, Phone Number, or Email; and Address While in the United States.

The System of Records Notice (SORN) for ESTA, last published on July 30, 2012, is being updated concurrently with this PIA to reflect the ESTA enhancements, including the revised eligibility questions and additional data elements on the ESTA application. The ESTA SORN’s “categories of individuals” is being amended to provide additional notice that U.S. citizen and lawful permanent resident information may be collected as a result of the new ESTA application data fields.

Due to the sensitive national security concerns necessitating this expanded information collection, DHS has determined that the updated ESTA SORN will become effective when it is displayed to the public, without a prior comment period. Despite the exigent circumstances requiring immediate publication and implementation of this new information collection, members of the public are still encouraged to submit comments on the updated SORN, and DHS will evaluate them to determine if any future changes should be made.

Privacy Impact Analysis

Authorities and Other Requirements

DHS/CBP will collect enhanced ESTA application information pursuant to Title IV of the Homeland Security Act of 2002, 6 U.S.C. § 201, *et seq.*; and the Immigration and Nationality Act (INA), as amended, including 8 U.S.C. § 1187 (h)(3)(A). These statutes authorize the Secretary of Homeland Security, in consultation with the Secretary of State, to “develop and implement a fully automated electronic travel authorization system to collect such biographical and other information as the Secretary of Homeland Security determines necessary to determine, in advance of travel, the eligibility of, and whether there exists a law enforcement or security risk in permitting, the alien to travel to the United States.” Implementing regulations for ESTA are contained in Part 217, title 8, Code of Federal Regulations.⁷

Characterization of the Information

⁶ See DHS Privacy Policy Guidance Memorandum 2007-01, Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons, January 7, 2009, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.

⁷ CBP collects a fee per travel authorization pursuant to section 217(h)(3)(B) of the INA (8 U.S.C. § 1187(h)(3)(B)) and provides part of the fee to the Corporation for Travel Promotion pursuant to the Travel Promotion Act of 2009, Pub. L. 111-145, 22 U.S.C. § 2131(d).



Information collected by ESTA is necessary to issue a travel authorization as reflected on the Form I-94W.

Mandatory Data Elements

With the publication of this PIA, DHS/CBP is notifying the public of new data elements added to the ESTA application and to the Form I-94W. The mandatory data elements that an applicant must now complete are indicated by a red asterisk on the ESTA website⁸ and listed below. The new data elements are indicated by an (*):

- Family name;
- First (given) name;
- Birth date (day, month, and year);
- Country of birth;
- Sex (male or female);
- Country of citizenship;
- Country where you live;
- Passport number;
- Passport issuing country;
- Passport issuance date (day, month, and year);
- Passport expiration date (day, month, and year);
- Other Names or Aliases;*
- Other Country of Citizenship;*
 - If yes, passport number on additional citizenship passport;*
- City of Birth;*
- Home Address;*
- Parents' Names;*
- Email;*
- Telephone Number;*
- National Identification Number;*
- Current Job Title;*
- Current or Previous Employer Name;*
- Current or Previous Employer Address;*
- Current or Previous Employer Telephone Number;*
- Emergency Point of Contact Information Name;*
- Emergency Point of Contact Information Phone;*
- Emergency Point of Contact Information Email;*

⁸ <https://esta.cbp.dhs.gov/esta/application.html?execution=e1s1>.



- U.S. Point of Contact Name;*
- U.S. Point of Contact Address;* and
- U.S. Point of Contact Telephone Number.*

Applicants are only required to provide one entry for each data element. When it is possible to provide more than one entry for a particular data element (e.g., multiple phone numbers or email addresses), applicants may, but are not required to, provide multiple entries.

Voluntary Data Elements

In addition to the new mandatory information and eligibility questions listed on Page 5, applicants have the option of providing additional voluntary data elements to complete their application. Optional data elements for ESTA have not changed since the initial 2008 information collection:

- City where you are boarding;
- Carrier information (carrier name and flight or vessel number); and
- Address while in the United States (address line 1 and 2, city, and state)

Revised Eligibility Questions

As noted, the PIA is also being updated to provide notice of revised and additional eligibility questions for ESTA applicants. CBP simplified and reformatted the eligibility questions to promote readability and understanding by the public. While some of the language has changed, the scope and substance of the eligibility questions remain the same. For example, CBP has eliminated ambiguous legal and medical terms of art and other confusing language that may not be easily understood by foreign nationals. Furthermore, CBP removed a question concerning withholding custody of a child from a U.S. citizen because the question affected only a miniscule percentage of ESTA applicants and thus represented an overreaching data collection. The only substantive addition to the eligibility questions asks whether an applicant has overstayed his or her previous admission period in the U.S., if applicable. This question helps identify foreign nationals who have unlawfully overstayed their previous period of admission.

ESTA applicants must now answer the following eight questions to complete their application:

- *Do you currently have any of the following diseases:*
 - *Chancroid*
 - *Gonorrhea*
 - *Granuloma Inguinale*
 - *Leprosy, infectious*
 - *Lymphogranuloma venereum*



- *Syphilis, infectious*
- *Active Tuberculosis*
- *Have you ever been arrested or convicted for a crime that resulted in serious damage to property, or serious harm to another person or government authority?*
- *Have you ever violated any law related to possessing, using, or distributing illegal drugs?*
- *Do you seek to engage in or have you ever engaged in terrorist activities, espionage or sabotage; or genocide?*
- *Have you ever committed fraud or misrepresented yourself or others to obtain, or assist others to obtain, a visa or entry into the United States?*
- *Are you currently seeking employment in the United States or you were you previously employed in the United States without prior permission from the U.S. government?*
- *Have you ever been denied a U.S. visa you applied for with your current or previous passport, or have you ever been refused admission to the United States or withdrawn your application for admission at a U.S. port of entry? If yes, when and where?*
- *Have you ever stayed in the United States longer than the admission period granted to you by the U.S. government?*

Privacy Impact Analysis: Related to Characterization of Information

Privacy Risk: There is a risk that the enhancements to the ESTA application are too broad to address current security threats.

Mitigation: The expansion of collected information on the ESTA application to support enhanced vetting efforts aligns with the original intent of ESTA, which is to identify individuals who pose a threat to the United States and are seeking to travel under the VWP, since the VWP allows individuals to travel to the United States outside of the traditional visa security process.

The new ESTA data elements were specifically chosen to target threats in a changing counterterrorism environment. DHS has determined that the new data fields will enhance DHS's ability to screen and more accurately and effectively identify travelers who pose a potential security risk to the homeland. Specifically, the inclusion of new data fields will provide a greater chance for DHS to identify foreign fighters with passports from VWP countries before they attempt to travel to the United States.

Uses of the System and the Information

DHS/CBP will continue to use the information included in the traveler's ESTA application to determine the eligibility of the foreign national to travel to the U.S. including



whether the visitor poses a law enforcement or security risk.⁹ The addition of the new data fields and updated eligibility questions on the ESTA application also enhance DHS/CBP's ability to decrease the number of inconclusive matches to derogatory records, providing benefits to both DHS/CBP and the applicant. Enhanced vetting capability allows DHS/CBP to mitigate existing security gaps that may arise due to the omission of these data elements from the current ESTA application process.

With the addition of the new data elements, the Department is better equipped to identify travelers of interest and distinguish them from legitimate travelers, thereby improving DHS's security capabilities while also facilitating the entry of lawful visitors. In addition to the enhanced vetting capability, the collection of additional name, dual citizenship, city of birth, home address, telephone number, parents' names, and national identification number data reduces the likelihood that an applicant with derogatory holdings will be automatically approved for a travel authorization. All of the requested employer data is used to identify ESTA applicants who associate with persons of interest due to law enforcement or security concerns.

The new data elements also provide benefits in reducing the number of inconclusive matches to derogatory records during the vetting process. Inconclusive matches ultimately result in a denial of the ESTA application and the applicant is directed to a U.S. Embassy or consulate to apply for a visa. Some of the new data elements added to the ESTA application will also be used as point of contact information. Home address and emergency point of contact information may also be used to notify designated individuals in the event of a catastrophic event such as the destruction or loss of an aircraft. U.S. point of contact information may also be used to notify a visitor of an event that may interfere with safe travel while in the U.S. DHS/CBP recognizes that VWP travelers may not have close U.S. ties or may be staying in multiple hotels while visiting the United States. In this instance, an ESTA applicant may provide the name of a first night hotel, friend, family member, or colleague in the United States to satisfy the U.S. point of contact requirement.

CBP will continue to collect the already mandatory information and eligibility questions on the ESTA application. The ESTA application vetting process remains the same for all VWP travelers despite the additional data collections and is addressed in greater detail in previous PIAs.¹⁰

Privacy Impact Analysis: Related to Uses of the System and the Information

⁹ See 8 U.S.C. 1187(h)(3).

¹⁰ See DHS/CBP/PIA-007(c) - Electronic System for Travel Authorization (ESTA) Update, published June 5, 2013; DHS/CBP/PIA-007(b) Electronic System for Travel Authorization (ESTA) - Internet Protocol Address and System of Records Notice Update, published July 18, 2012; DHS/CBP/PIA-007(a) Electronic System for Travel Authorization (ESTA) Fee and Information Sharing Update, published July 18, 2011; DHS/CBP/PIA-007 Electronic System for Travel Authorization, published June 2, 2008.



Privacy Risk: Additional information collected by the ESTA application may be used for purposes inconsistent with the original collection.

Mitigation: DHS will handle the new information in the same manner and for the same purposes as it already does for existing ESTA information. The additional questions will improve DHS's ability to identify individuals with links to terrorist activities who might have gone undetected without the additional information. DHS has determined that the additional data fields will make DHS screening more accurate, enhance the Department's ability to conduct identity resolution, and help DHS pinpoint security threats.

Retention

The DHS retention period for ESTA has not changed. CBP retains ESTA application data for no more than three years in an active database (one year beyond the ESTA authorization expiration date) and twelve years in archive status.

Internal Sharing and Disclosure

No changes have been made to internal sharing and disclosure.

External Sharing and Disclosure

DHS shares ESTA information in bulk with other federal counterterrorism partners (e.g., the National Counterterrorism Center), and DHS may share ESTA on case-by-case basis to appropriate state, local, tribal, territorial, foreign, or international government agencies. Existing external information sharing and access agreements will continue, and will now include the expanded categories of individuals and records noted above.

This sharing takes place after DHS determines that the recipient has a need to know the information to carry out functions consistent with the exceptions under the Privacy Act of 1974, 5 U.S.C. § 552a(b), and the routine uses set forth in the ESTA SORN. Additionally, for ongoing, systematic sharing, DHS completes an information sharing and access agreement with federal partners to establish the terms and conditions of the sharing, including documenting the need to know, authorized users and uses, and the privacy protections for the data.

Notice

The ESTA SORN was last published in the Federal Register on July 30, 2012, 77 FR 44642. Concurrent with this PIA update, CBP is publishing a newly updated SORN in the Federal Register to provide notice of revised categories of records and the additional categories of individuals covered by the ESTA system to account for the revised eligibility questions and additional data elements collected on the ESTA application.

Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals, particularly U.S. Persons (e.g., U.S. or emergency points of



contact), may not be aware that their information may be recorded in ESTA and may be used for vetting an ESTA applicant. Furthermore, these individuals will not have an opportunity to have their information removed from evaluation and/or disassociated with an ESTA application.

Mitigation: There is no opportunity to notify individuals, including U.S. Persons, who may be named in an ESTA application by the ESTA applicant or to provide an opportunity for those individuals to have their information removed from evaluation and/or disassociated with an ESTA application. To partially mitigate this risk, DHS is providing notice to the public of this new information collection by publication of the PIA and the accompanying SORN to provide as much transparency into its operations as possible.

If an individual believes that DHS may have information about him or her as part of the expanded ESTA application, individuals are encouraged to follow the individual access, redress, and correction procedures described below.

Individual Access, Redress, and Correction

No changes have been made to access, redress, and correction of personally identifiable information in ESTA. However, CBP updated the address to which individuals should submit their requests for access, redress, and correction.

Under the Privacy Act and the Freedom of Information Act (FOIA), individuals may request access to the information they provide which is maintained in the applicable CBP system of record. Proper written requests under the Privacy Act and FOIA should be addressed to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
90 K Street NE, 9th Floor
Washington, DC 20002

Requests for access should conform to the requirements of 6 CFR Part 5, which provides the rules for requesting access to Privacy Act records maintained by DHS. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

Applicants denied a travel authorization to the U.S. via ESTA may still apply for a visa from the U.S. Department of State. General complaints about treatment or requests for redress can be made to the DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip. Generally, if a traveler believes



that CBP actions are the result of incorrect or inaccurate information, then inquiries should be directed to:

CBP INFO Center
OPA - CSC - Rosslyn
U.S. Customs and Border Protection
1300 Pennsylvania Ave, NW
Washington, DC 20229

Technical Access and Security

No changes have been made to technical access or security.

Technology

No changes have been made to the existing technology.

Responsible Officials

Suzanne Shepard, Director ESTA
U.S. Customs and Border Protection
Department of Homeland Security

John Connors, CBP Privacy Officer
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security